資通安全管理法
教育體系之法遵說明

教育部資訊及科技教育司

108年09月20日

簡報大綱

- 資通安全管理法
- 資通安全責任等級
- 資通安全維護計畫

資通安全管理法

資通安全管理法

- 總統107年6月6日公布**資通安全管理法**。
- 行政院107年11月21日發布相關子法：
  - **資通安全管理法施行細則**
  - **資通安全責任等級分級辦法**
  - **資通安全事件通報及應變辦法**
  - **特定非公務機關資通安全維護計畫實施情形稽核辦法**
  - **資通安全情資分享辦法**
  - **公務機關所屬人員資通安全事項獎懲辦法**
- 行政院107年12月05日函定自**108年1月1日施行**。

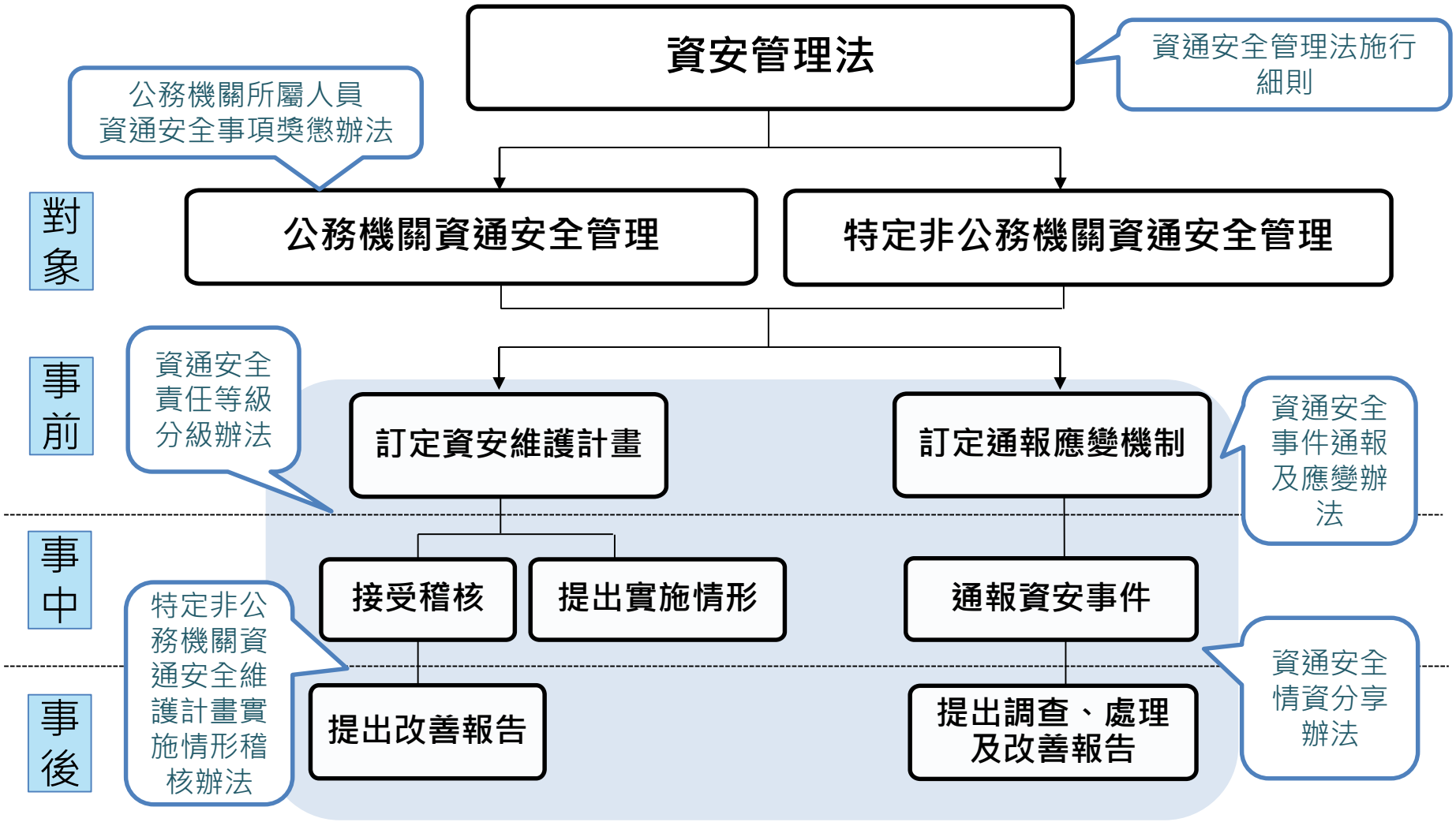
教育體系資通安全相關行政規則

- 政府機關（構）資通安全責任等級分級作業規定
  - 行政院104年1月20日院臺護字第1040121116號函修正發布
- 教育部與所屬機關(構)及學校資通安全責任等級分級作業規定
  - 教育部104年7月13日臺教資(四)字第1040059997號函發布
- 資訊系統分級與資安防護基準作業規定
  - 行政院104年7月31日院臺護字第1040141147號函
- 國家資通安全通報應變作業綱要
  - 行政院105年8月24日院臺護字第1050173756號函修正發布

教育體系資通安全相關行政規則

- ~~政府機關（構）資通安全責任等級分級作業規定~~
  - 行政院108年3月5日院臺護字第1080166960號函停止適用
- 教育體系資通安全責任等級分級作業規定(草案)
- ~~資訊系統分級與資安防護基準作業規定~~
  - 行政院108年3月5日院臺護字第1080166960號函停止適用
- ~~國家資通安全通報應變作業綱要~~
  - 行政院108年3月5日院臺護字第1080166960號函停止適用
- 臺灣學術網路各級學校資通安全通報應變作業程序
  - 教育部108年5月2日臺教資(四)字第1080063494號函訂定

資通安全管理法架構


資安管理法
資通安全管理法施行細則
公務機關所屬人員資通安全事項獎懲辦法
對象
公務機關資通安全管理
特定非公務機關資通安全管理
事前
資通安全責任等級分級辦法
訂定資安維護計畫
訂定通報應變機制
資通安全事件通報及應變辦法
事中
接受稽核
提出實施情形
通報資安事件
特定非公務機關資通安全維護計畫實施情形稽核辦法
事後
提出改善報告
提出調查、處理及改善報告
資通安全情資分享辦法

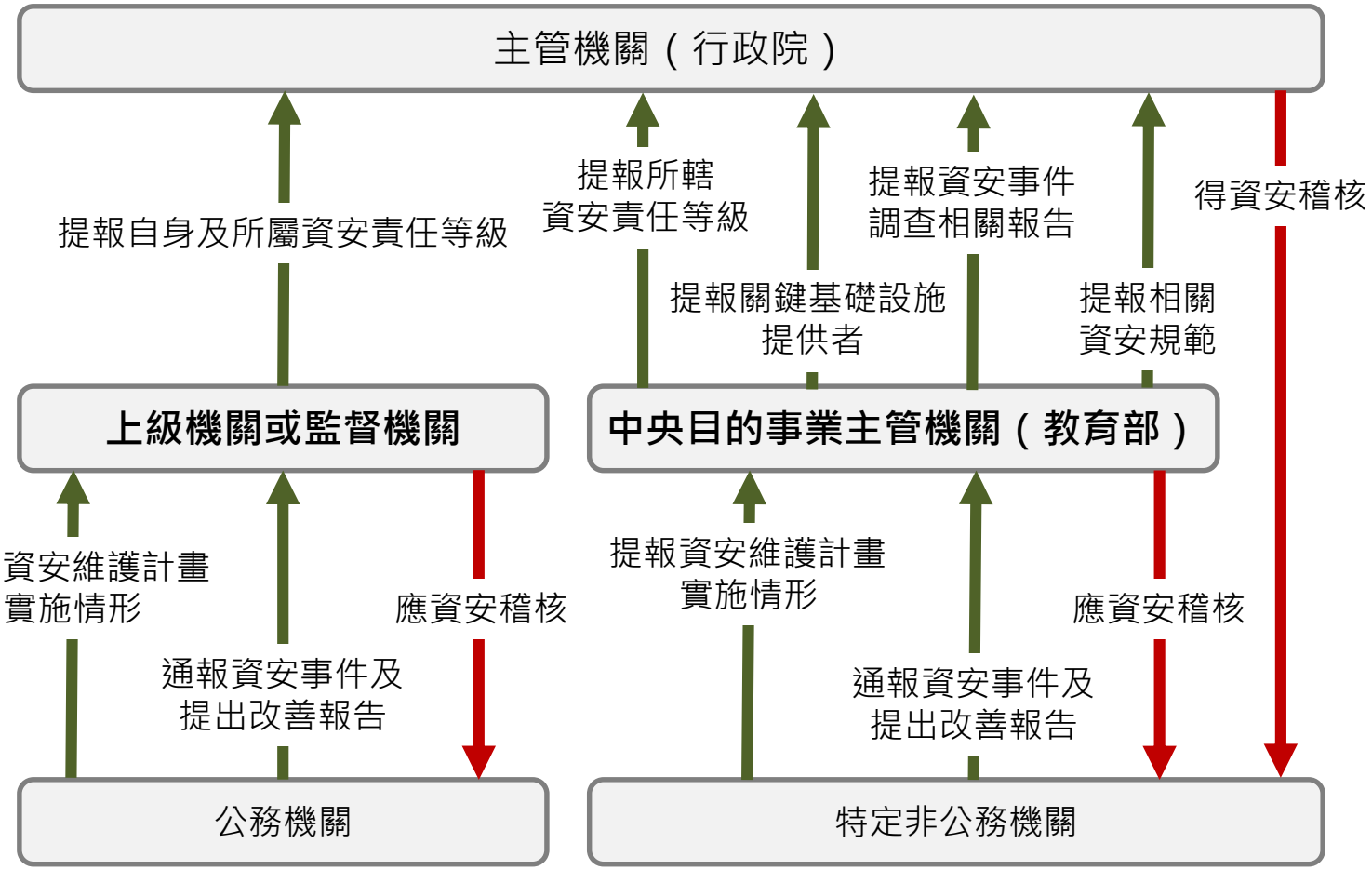
立法目的與規範對象

- 立法目的
  - 為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益。
- 規範對象
  - 公務機關
    - 依法行使公權力之中央、地方機關（構）或公法人。
    - 公立學校除屬軍事機關之國防部所屬學校外，均屬本法規定之公務機關。（行政院秘書長108年5月10日院臺護字第1080013640號函釋）
  - 特定非公務機關
    - 關鍵基礎設施提供者。
    - 公營事業、政府捐助之財團法人。

教育體系資通安全管理法適用對象

- 公務機關
  - 教育部及所屬機關（構）、國家運動訓練中心
  - 各級公立學校及其附設機構（農林場、醫院等）
- 特定非公務機關
  - 教育部主管政府捐助之財團法人
    - 財團法人大學入學考試中心基金會
    - 財團法人高等教育評鑑中心基金會
    - 財團法人高等教育國際合作基金會
    - 財團法人私立學校興學基金會
    - 財團法人社教文化基金會等12家財團法人。

角色與權責



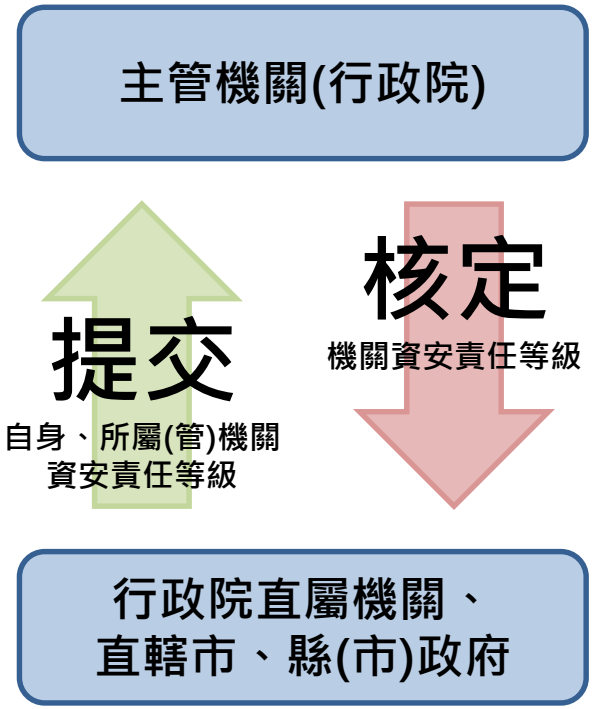
- 設置資安長
- 訂定及實施資安維護計畫
- 訂定資安事件通報及應變機制

- 訂定及實施資安維護計畫
- 訂定資安事件通報及應變機制

資通安全責任等級

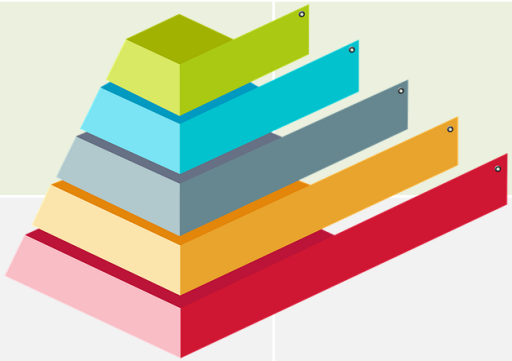
資通安全責任等級提交

- **提交機關**應每2年提交所屬責任等級，報行政院核定。
  - 行政院直屬機關（教育部）
    - 部屬機關、機構
    - 國立大專校院及其附設機構
    - 國立高級中等以下學校
    - 教育部主管政府捐助之財團法人
  - 各直轄市、縣（市）政府
    - 教育網路中心（二級單位）
    - 直轄市、縣（市）立各級學校



- 資通安全責任等級分級辦法第3條

資安責任等級分級原則

	業務	資通系統	個資檔案持有	層級
A級	國家機密、外交、國防或國土安全事項	維運**全國性民眾服務**或**跨公務機關共用性**資通系統	**全國性民眾或公務員**個人資料檔案之持有	**公立醫學中心**
B級	公務機關捐助、資助或研發**敏感科學技術資訊**之安全維護及管理	維運**區域性、地區性民眾服務**或**跨公務機關共用性**資通系統	**區域性或地區性民眾**個人資料檔案之持有	公立區域醫院或地區醫院
C級		維運**自行或委外開發**資通系統		
D級		**未維運**自行或委外開發之資通系統，自行辦理資通業務		
E級		無資通系統且未提供資通服務，**全部資通業務由其上級機關兼辦代管**。		

資通安全責任等級分級辦法第4條至第8條

教育體系資安責任等級核定

- 依行政院108年7月24日院臺護字第1080180748號資通安全責任等級核定函，教育體系各單位責任等級核定如下：

	政府機關構	學校	學校附設機構	財團法人	合計
A級	1	0	2	1	4
B級	2	45	8	0	55
C級	13	4	1	9	27
D級		158	3	1	162
E級			1	1	2
合計	16	207	15	12	250

（不含直轄市、縣市立高級中等以下學校）

分級作業辦法應辦事項-管理面

辦理事項	辦理內容	A	B	C
資通系統分級及防護基準	完成資通系統分級，並完成防護基準；每年至少檢視一次妥適性	1年內		2年內
ISMS之導入及通過公正第三方之驗證	2年內**全部核心資通系統**導入資訊安全管理系統。	3年內完成第三方驗證；並持續維持期驗證有效性。		O*
業務持續運作演練	**全部核心資通系統**	每年1次	每2年1次	
辦理內部資通安全稽核		每年2次	每年1次	每2年1次
資通安全專職(責)人員（1年內）		4人	2人	1人*
資安治理成熟度評估（公務機關）		每年1次		X
限制使用危害國家資通安全產品		除因業務需求且無其他替代方案外，**不得採購及使用主管機關核定**之廠商生產、研發、製造或提供之**危害國家資通安全產品**（目前尚未核定）。		

分級作業辦法應辦事項-技術面

辦理項目	辦理內容	A	B	C
安全性檢測 全部核心資通系統*	網站安全弱點檢測	每年2次	每年1次	每2年1次
	系統滲透測試	每年1次	每2年1次	
資通安全健診*	網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆設定檢視	每年1次	每2年1次	
資通安全威脅偵測管理機制*	完成威脅偵測機制建置，並持續維運	1年內		X
	依行政院指定方式提交監控管理資料	O	O	X
資通安全防護 （啟用，並持續使用及適時進行軟、硬體之必要更新或升級）	防毒軟體、網路防火牆、具有郵件伺服器者，應備電子郵件過濾機制	1年內		
	IDS/IPS、具有對外服務之核心資通系統者，應備應用程式防火牆（WAF）	1年內		X
	APT攻擊防禦	1年內	X	
政府組態基準 （GCB）	依主管機關公告之項目，完成GCB導入作業，並持續維運（公務機關）	1年內		X

分級作業辦法應辦事項-認知與訓練

辦理事項	辦理內容	A	B	C
資通安全教育訓練	**資通安全專職人員***	每人每年至少接受12小時以上之**資通安全專業課程**訓練或**資通安全職能**訓練。		
	資通安全專職人員以外之**資訊人員**	每人每2年至少接受3小時以上之**資通安全專業課程**訓練或**資通安全職能**訓練，且每年接受3小時以上之**資通安全通識**教育訓練。		
	一般使用者及主管	每人每年接受三小時以上之**資通安全通識**教育訓練。		
資通安全專業證照及職能訓練證書	初次受核定或等及變更後之一年內，資通安全專職（責）人員總計應持有之**資通安全專業證照**，並持續維持證照之有效性	4張以上	2張以上	1張以上
	資通安全專職人員總計應持有之**資通安全職能評量證書**，並持續維持證照之有效性（公務機關）	4張以上	2張以上	1張以上

分級作業辦法應辦事項-D、E級

面向	辦理項目	辦理細項	D	E
技術面	資通安全防護	防毒軟體、網路防火牆、具有郵件伺服器者，應備電子郵件過濾機制	1年內	X
認知與訓練	資通安全教育訓練	一般使用者及主管，每人每年至少接受之一般資通安全教育訓練	每人3小時	

公立高級中等以下學校因應措施

責任等級		C級	依分級辦法第10條第4款調整為D級	D級	E級
認定原則	**核心資通系統**	**110年仍自行維運者**	已向上集中或規劃109年底前集中者	已向上集中	已向上集中
	非核心資通系統	**自行維運**	**自行維運**	已向上集中	已向上集中
	資通業務	**自行辦理**	**自行辦理**	**自行辦理**	由上級代管

公立學校資訊資源向上集中計畫

- **核心資通系統**：指資通安全管理法施行細則第七條第二項之核心資通系統（如**官方網站**、應用於全校校務行政及教學等重要業務之**電子郵件服務系統**、**網域名稱系統**、**公文系統**、**校務行政系統**或其他涉及**持有學生或教職員個人資料檔案資通系統**等）。
- 非核心資通系統需與核心資通系統有明確區隔（不得直接存取）。

公立高級中等以下學校因應措施

責任等級		C級	依分級辦法第10條第4款調整為D級	D級	E級
資通系統分級及防護		✓	✓		
核心系統	資訊安全管理系統（ISMS）	需導入			
	業務持續運作演練及安全性檢測（弱掃、滲透測試）	2年一次			
內部稽核		✓	內部檢查		
資通安全健診		✓	△		
資通安全防護（防毒、防火牆、郵件過濾）		✓	✓	✓	
資安人員	配置	專職人員	專責人員		
	資通安全專業證照及 資通安全職能評量證書	✓			
	資通安全專業課程訓練	12小時	12小時		
一般人員通識教育訓練		3小時	3小時	3小時	3小時

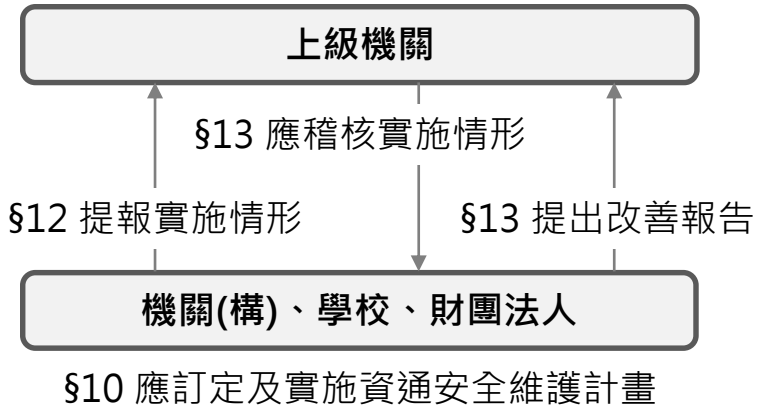
應辦事項配套措施

應辦單位	辦理項目		因應措施
A、B級	資通安全威脅偵測管理機制		臺灣學術網路連線單位可結合**臺灣學術網路資安監控系統(南、北SOC, Mini-SOC)**進行威脅偵測機制。
A、B、C級	核心資通系統	網站安全弱點檢測	由**成功大學網站防護團隊**協助辦理。
		滲透測試	教育體系資安檢核技術服務計畫協助辦理。
	資通安全健診		請**北、南區學術資訊安全維運中心**協助辦理相關教育訓練課程。 高級中等以下學校委請教育體系資安檢核技術服務計畫團隊協助開發相關工具及SOP
	資通安全專業證照		委託教育機構資安驗證中心(國立中興大學)開設ISO 27001:2013 LA、BS 10012:2017 LA 證照專班。
	資通安全職能評量證書		後續教育體系委託政治大學協助辦理相關教育訓練，由國家資通安全會報技術服務中心考試評量。

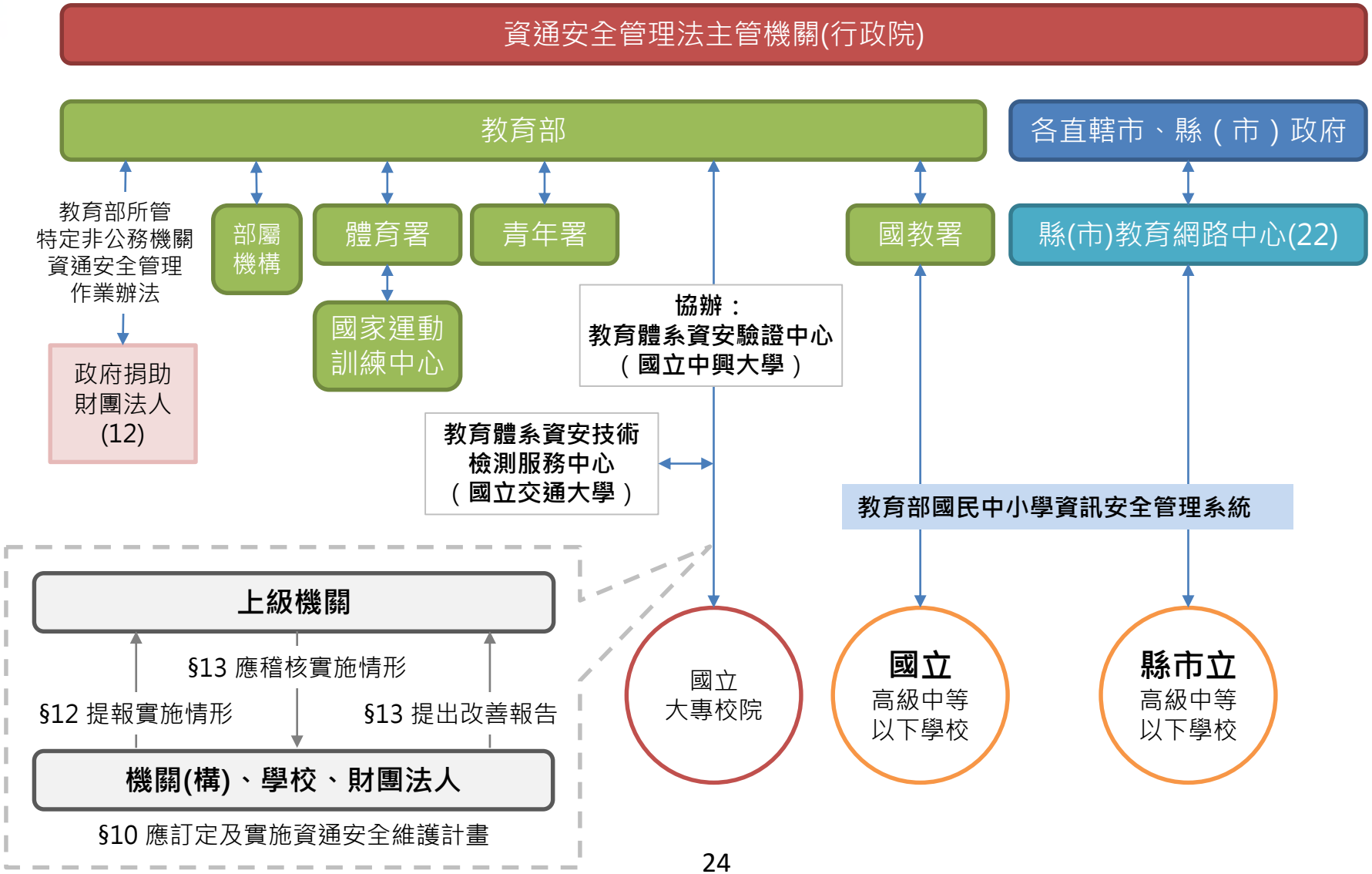
資通安全維護計畫

資通安全維護計畫

- **公務機關應訂定及實施資通安全維護計畫。**
- （資通安全管理法第10條）
- **公務機關應每年向上級提出資通安全維護計畫實施情形。**
  （資通安全管理法第12條）
- **公務機關應稽核其所屬機關之資通安全維護計畫實施情形。**
  （資通安全管理法第13條）



教育體系稽核作業


資通安全管理法主管機關(行政院)
教育部
各直轄市、縣（市）政府
教育部所管特定非公務機關資通安全管理作業辦法
政府捐助財團法人(12)
部屬機構
體育署
青年署
國家運動訓練中心
國教署
縣(市)教育網路中心(22)
協辦：教育體系資安驗證中心（國立中興大學）
教育體系資安技術檢測服務中心（國立交通大學）
教育部國民中小學資訊安全管理系統
上級機關
§13 應稽核實施情形
§12 提報實施情形
§13 提出改善報告
機關(構)、學校、財團法人
§10 應訂定及實施資通安全維護計畫
國立大專校院
國立高級中等以下學校
縣市立高級中等以下學校

教育體系稽核作業

- 大專校院
  - 委託「教育機構資安驗證中心」協助辦理相關稽核作業。
    - 制度面：教育部本部。
    - 管理面：教育機構資安驗證中心（國立中興大學）。
    - 技術面：教育體系資安技術檢測服務中心（國立交通大學）。
- 高級中等以下學校
  - 補助新北市政府教育局開發「資訊安全管理系統」。
    - 訂定維護計畫：學校填報上傳「資通安全維護計畫」。
    - 學校提報實施情形：學校填報實施情形題目。
    - 稽核實施情形：評量人員線上評量審查，到校輔導訪視。

感謝指導